

AMENDMENT 2 FOR RFP NUMBER 0A1049

DATE AMENDMENT ISSUED: November 6, 2008

The State of Ohio, through the Department of Administrative Services, for the Office of Budget and Management and the Office of Information Technology within the Department of Administrative Services is requesting proposals for:

PeopleSoft Services/Project Services

INQUIRY PERIOD BEGINS: October 6, 2008
INQUIRY PERIOD ENDS: November 10, 2008
OPENING DATE: November 17, 2008
OPENING TIME: 1:00 P.M.
**OPENING LOCATION: Department of Administrative Services
General Services Division
IT Procurement Services
Bid Desk
4200 Surface Road
Columbus, Ohio 43228-1313**

INTENT TO RESPOND DUE: October 9, 2008

PRE-PROPOSAL CONFERENCE DATE: October 15, 2008 @ 1:00 P.M.

The attached is an Amendment for the RFP listed above. Please use the replacement page(s) contained in the Amendment to replace the corresponding page(s) previously in the RFP.

Specifications and requirements that have been revised are surrounded by bolded double asterisks and, when applicable, strikethrough.

PART ONE: EXECUTIVE SUMMARY

Purpose. This is a Request for Competitive Sealed Proposals ("RFP") under Section 125.071 of the Ohio Revised Code (the "Revised Code") and Section 123:5-1-8 of the Ohio Administrative Code (the "Administrative Code"). The Office of Budget and Management and the Office of Information Technology within the Department of Administrative Services has asked the Department of Administrative Services to solicit competitive sealed proposals ("Proposals") for Managed Services, the Shared Services Implementation and Ongoing Project Services (the "Work"), and this RFP is the result of that request. This RFP combines several closely related services needed by the State of Ohio (the "State"). While the State strongly desires a single vendor solution, it is the intent of the State to conduct the evaluation and selection processes in a manner that provides the flexibility for considering multiple vendor solutions for the Work, which may result in two contractor awards. If the State elects to award a contract for the Work, two contracts with either a single or two contractors will result.

If a suitable single vendor solution is made in response to the Work, the State, through the Department of Administrative Services (DAS), may enter into a single or multiple contracts (the "Contract") to have the selected offeror (the "Contractor") perform all or part of the Work. Multiple contracts with a single Contractor may be necessary to award portions of the Work at different times within the RFP process. The State believes there may be significant benefits to awarding the Work to a single Contractor. These benefits will be considered by the State during the evaluation and selection process.

Alternatively, the State may determine that it is in its best interests to award the Work to different Contractors. Therefore, if a suitable offer is made in response to the Managed Services portion of this RFP, the State, through DAS, may enter into a separate contract (the "Contract") to have the selected Managed Services offeror (the "Contractor") perform all or part of the Work described within the scope of Managed Services. Similarly, if a suitable offer is made in response to the Shared Services Implementation portion of this RFP, the State, through DAS, may enter into a separate contract (the "Contract") to have the selected Shared Services Implementation offeror (the "Contractor") perform all or part of the Work described within the Shared Services Implementation scope. The Ongoing Project Services for post implementation, ongoing or future projects may be incorporated in one or both Contracts.

All offerors submitting Proposals must submit a single proposal containing an offer for all of the Work. Submitting a Proposal for only a portion of the Work is not acceptable and will result in the incomplete Proposal not being considered. This RFP provides details on what is required to submit a Proposal for the Work, how the State will evaluate the Proposals, and what will be required of each Contractor in performing the Work.

This RFP also gives the estimated dates for the various events in the submission process, selection process, and performance of the Work. While these dates are subject to change, prospective offerors must be prepared to meet them as they currently stand.

The Term of this contract is from award date until the work is completed to the satisfaction of the State and the Contractor is paid or June 30, 2009, whichever is sooner. The State may renew the Contract(s) for up to three additional two-year terms subject to the Ohio General Assembly appropriating funds in each new biennium; however, the Contractor may terminate the Contract(s) without penalty as of June 30, 2013 ****by providing 180 days prior written notice to the State****. The State may renew this Contract in the next biennium by issuing written notice to the Contractor of the decision to do so. This expiration and renewal procedure also will apply to the end of any subsequent biennium during which the work continues, subject to the State's approval and subject to the Contractor's right to terminate the Contract(s) as of June 30, 2013.

Beginning on the 3rd anniversary of the Contract date and running 30 days thereafter, the State has the right to terminate the Contract by giving at least 30 days notice without penalty.

6.5.1 Software Licensing Considerations

Offerors are instructed to consider and address the following considerations with respect to software licensing for Statement(s) of Work contained in this RFP.

1. Where software is existing and licensed by the State as represented herein, the State will continue to retain ownership and maintenance obligations with respect to this software in accordance with existing agreements with 3rd party software vendors (e.g., PeopleSoft, Oracle, existing toolsets);
2. Where software is specified as part of this RFP which does not exist within the State, or is otherwise not available or licensed by the State, is not provided as a included cost in the offeror's proposal, and will be required for the State to perform these services over the term of the agreement (and if required post agreement), these software elements are to be specified with costs in the Cost Summary and an accompanying software bill of materials (e.g., database licenses, middleware, job schedulers etc) ;
3. Where software is provided as part of this RFP which is in support of the delivery of Managed Services and is not required to be licensed to the State and/or transferred to the State upon conclusion of the agreement, offeror is to provide this software as a priced element as part of their Managed Service offering (e.g., service desk tools, inventory and SL reporting tools, asset tracking etc). Regardless of ownership, the State retains all rights to the underlying State data and reports contained in these software elements;
4. Where software is required as part of the delivery of the Shared Services implementation that requires the State to license this software to support the implementation/development effort (e.g., code versioning, testing, development tools etc), offeror is to specify these software elements with costs in the Cost Summary. Offerors should record the costs in rows 97 or 98 of the Cost Summary and provide a detailed bill of materials that supports the required software costs inclusive of maintenance, updates and upgrades. The State is under no obligation to accept offeror provided pricing, and reserves the right to license this software directly from the OEM software provider at its sole discretion.
5. Where software is required as part of the delivery of the Shared Services implementation that does not require the State to license this software to support the implementation/development effort (e.g., vendor enablers, tools, methodologies and frameworks), offeror is to include these software elements in Cost Summary. Offerors should record the costs in rows 97 or 98 of the Cost Summary and provide a detailed bill of materials that supports the required software costs inclusive of maintenance, updates and upgrades. The State is under no obligation to accept offeror provided pricing, and reserves the right to license this software directly from the OEM software provider at its sole discretion.

6.12.1 Data Archive and Purge Considerations

Based on experience running the PeopleSoft environments since the implementation of OAKS, the State has determined that there may be a requirement for accommodating the archive and purge of historical or obsolete data from the production environments. At a high level, the rationale for implementing archive and purge functionality is to ensure that: the overall performance characteristics of the system is not compromised processing or accommodating historical data; the overall costs associated with storage, backup and maintenance of historical data are cost effective; and requirements for creating subsets of data to support the development, testing and training of projects such as the Shared Services implementation addressed in this RFP in Section 10.

Based on the high level requirements outlined above, the State has evaluated various methods to accomplish the archive and purge functionality including: the development of customized scripts to facilitate the extraction and migration of data to online, offline or purge data stores; and the purchase and subsequent implementation of commercial packages available on the marketplace from vendors such as IBM, HP and Applimation. Based on the review of the available packages and a custom set of scripts, the State is contemplating the development of custom scripts to achieve the archive and purge requirements but due to the timing of this RFP, and the probability that offerors may have pre-existing tools, techniques or methods, the State requests that offerors propose their preferred method for managing general archive and purge requirements in their PeopleSoft managed services environments. Offerors are required to include a high level description of capabilities, features, configuration and limitations of their provided toolset, any underlying assumptions as to the basis for provision of these functions, and any incremental pricing associated with the delivery and implementation of these capabilities.

Offerors are to note that these functions are not required if, in the view of the offeror: 1) overall Service Levels can be achieved, particularly those pertinent to application performance; 2) storage costs are not significant as to warrant the provision of these functions in consideration of cost to deploy and manage these functions relative to the cost of the underlying storage; and 3) the data sub-setting requirements of the Shared Services project and other similar projects that may arise in the future can be achieved.

6.12.2 Data Masking and Information Privacy in Non Production Environments

The State has a requirement for all non-production environments (e.g., development, testing, training) that require production data refresh from time to time as outlined in the table in Section 6.1. Elements of production data that require protection under information privacy regulations such as Social Security numbers, bank account information and other sensitive data must be protected in these environments. As a result of these requirements, and as highlighted by certain elements of the Shared Services implementation, the State has conducted a preliminary analysis and several vendor driven proof-of-concepts and demonstrations as part of the formulating a strategy to achieve these requirements including a preliminary review of the available packages from Applimation and IBM, features available in Oracle DBMS 10G.

Due to the timing of this RFP, and the probability that offerors may have pre-existing tools, techniques or methods, the State requests that offerors propose their preferred method for achieving data masking or private data in their PeopleSoft managed services environments. The State has no plans or preferences with respect to selecting or implementing a package or data masking technique prior to the award of a Managed Services contract. Offerors are required to include a high level description of capabilities, features, configuration and limitations of their provided toolset or approach, any underlying assumptions as to the basis for provision of these functions, and any incremental pricing associated with the delivery and implementation of these capabilities.

- Contractor will provide State an inventory of resources (or resource full time equivalents) then performing work under the Managed Services statement of work to assist the State in determining the appropriate resourcing and skill model required for the State or a State contracted Third Party to assume the services as provided by the Contractor at the time of termination. This resource inventory will include (at a minimum); full-or part time equivalent resource models; skill and experience levels; education or technical skill certification levels required; and other mutually agreeable and pertinent information for the State to assemble or source the capabilities to perform the work described herein upon termination of the Contract post transition of services. Contractors are to note State does not require names of individuals as part of fulfilling this requirement.
- ****In addition to the requirements in this section, in the event of a transfer of services back to the State and at the State's sole discretion, Contractor will design and implement a training program to State employees designed to convey operational and technical knowledge associated with the ongoing operation of the in-scope applications and systems, conduct knowledge and documentation transfers for the then current operational processes and tasks and work to ensure an overall continuity of services until such time as State employees can reasonably perform the roles in keeping with service levels and other operational quality, timeliness and accuracy considerations associated with the delivery of the service. These services will be priced utilizing the then current Contractor rate card at the time of the request and as approved by the State.****

8.12.3 Standards

The terminated or expired Services are transferred to the State or its successor(s) in an efficient and orderly manner.

The impact on the State's business (including its personnel and customers) and the internal and Third Party IT-related costs incurred by the State in transferring the Terminated Services are acceptable to the State under the circumstances.

The Terminated Services continue to be performed by Contractor without disruption or deterioration until the transfer has occurred: (i) consistent with the terms and conditions of this Contract, or (ii) except as approved by the State.

Any disruption or deterioration of the remaining Services following the transfer (except as approved by the State or included in the Termination Assistance Plan) to the extent the same is within the control of Contractor and as agreed with the State.

In an effort to facilitate transition of responsibilities, the Key Management Position obligations in the Governance Section 7.0 will continue to apply during the agreed Termination Assistance Period.

8.12.4 Termination Assistance Plan

The contents of Termination Assistance Plan will include, unless otherwise agreed, the services, functions, and activities as defined below:

- Documentation of existing and planned Projects and support activities.
- Identification of the Services and related positions or functions that require transition and a schedule, plan and procedures for the State or its designee assuming or reassuming responsibility.
- Description of actions to be taken by Contractor in performing Termination Assistance.
- Description of how the transfer of (i) relevant information regarding the Services, (ii) resources (if any), (iii) operations and (iv) contracts (if any) will be achieved.
- Description in detail of any dependencies on the successors necessary for Contractor to perform the Termination Assistance Services (including an estimate of the specific Contractor staffing required).
- Inventory of documentation and work products required to facilitate the transition of responsibilities.
- Assist the State in the identification of significant potential risk factors relating to the transition and in designing plans and contingencies to help mitigate the risk.
- Set out the timeline for the transfer of each component of the terminated Services (including key milestones to track the progress of the transfer).
- Define a schedule and plan for Contractor's return to the State of (i) the State Service locations then occupied by Contractor (if any), and (ii) the State Confidential Information, the State Data, documents, records, files, tapes and disks in Contractor's possession.

8.12.5 Termination Management Team

Contractor will provide a senior Project manager who will be responsible for Contractor's overall performance of the Termination Assistance Services and who will be the primary point of contact for the State in respect of the Termination Assistance Services during the Termination Assistance Period.

The State will appoint a senior Project manager who will be the primary point of contact for Contractor during the Termination Assistance Period. Additionally, the State may appoint a Transformation Team that would be responsible for the review of then current services provided by the Contractor and work to facilitate an orderly transition of services.

8.12.6 Operational Transfer

Contractor will perform the activities reasonably required to help effect a smooth and orderly transfer of operational responsibility for the Terminated Services.

Facilitating access to the State source code, object code, object and production libraries, reference files, field descriptions, record layouts and technical specifications along with run documentation for the State software then in Contractor's possession including tools, scripts, run books, production schedules and procedures as required to support the in-scope Applications which may be used in training, knowledge transfer, sizing assessments, operational reviews and other uses required by the state at the time of Transfer.

Cooperating with the Successors in conducting migration testing.

Providing the State owned documents and information related to the functionality, program code, data model and data base structure, and access methods for the in-scope Applications and manual and automated processes used for the State, within the possession or control of Contractor, and reviewing such processes, documents and information with the Successor as reasonably requested.

Cooperating with the State's test plans, back out procedures, and contingency plans as part of the migration of Terminated Services.

After the transfer of the provision of Terminated Services to the State, its designee(s), or both, providing additional assistance as reasonably requested by the State to facilitate continuity of operations, through the end of the Termination Assistance Period.

8.13 Additional Managed Services Terms and Conditions

The following provisions are applicable to this Managed Services SOW and supplement, but do not replace the provisions contained in Attachment Four. The provisions in Attachment Four continue in full force and effect for this Managed Services SOW and all other provisions of the Contract.

8.13.1 Audit

(a) Onsite Operational and Financial Examinations. To assist the State in its activities related to oversight of Contractor in the performance of the Contract, in addition to the examinations that occurred prior to the execution of this Contract, subsequent to the Effective Date of this Contract, the State, or its agent, may conduct onsite operational and financial examinations of Contractor.

(i) The onsite examinations may include, without limitation, verification that business is conducted as represented by Contractor at all sites where it performs Managed Services or Disaster Recovery for the State; Contractor's facilities are adequate to support claims of staffing, services performed and inventory housed; and the facilities provide adequate security for staff, functions performed and services rendered. This examination may include verification that Contractor has adequate information security compliance policies and procedures.

(ii) The financial examination may include, without limitation, a review of Contractor's current balance sheet; its most recent annual report; up to three (3) years of third party audits; tax returns for the previous three (3) years; and all documentation supporting employee bonds and insurance policies of Contractor.

(b) Consent to Examinations.

(i) By execution of this Contract, Contractor consents to the examinations described in these provisions and consents to such examinations being conducted by the State or its agent.

(ii) The State may conduct such examinations from time to time during the Term of this Agreement and the consent to the examinations provided by Contractor shall be a continuing

consent to conduct the examinations periodically in the State's discretion during the Term of this Contract.

(c) Right to Terminate.

(i) In the event the State determines in its sole discretion that the results of any examination of Contractor is unsatisfactory per the requirements of the Contract and not remedied within a 30 day period following notice from the State, the State may terminate this Agreement, in part or in full.

(ii) If the Contractor fails to satisfy the requirements of the State with regard to security of information, or if an examination reveals information that would result in a continuing contractual relationship that causes the State to be in violation of any law, the State may terminate this Contract immediately without notice.

(iii) If Contractor fails to satisfy the requirements of the State with regard to matters not related to those discussed in paragraph (c) (i) or (ii), the State will provide Contractor with notice and an opportunity to cure the failure within thirty (30) days. If the failure is not cured by Contractor within such thirty (30) day period, the State may terminate this Contract without further notice.

8.13.2 Criminal Background Check of Personnel

Contractor agrees that (1) it will conduct third-party criminal background checks on Contractor personnel who will perform Sensitive Services (as defined below), and (2) no Ineligible Personnel will perform Sensitive Services under this Agreement. "Ineligible Personnel" means any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, or money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a Specially Designated National, or (b) has been convicted of a felony. "Sensitive Services" means those services that (i) require access to Customer/Consumer Information, (ii) relate to the State's computer networks, information systems, databases or secure facilities under circumstances that would permit modifications to such systems, or (iii) involve unsupervised access to secure facilities ("Sensitive Services"). Upon request, Contractor will provide written evidence that all of Contractor's personnel providing Sensitive Services have undergone a criminal background check and are eligible to provide Sensitive Services. In the event that Contractor does not comply with the terms of this section, the State may, in its sole and absolute discretion, terminate this Contract immediately without further liability.

8.13.3 Confidentiality

A. Protection of State Data. To protect State Data as described in this Managed Services SOW, in addition to its other duties regarding State Data, Contractor shall:

1. Maintain in confidence any personally identifiable information ("PI") it may obtain, maintain, process, or otherwise receive from or through the State in the course of the Agreement;

2. Use and permit its employees, officers, agents, and independent contractors to use any PI received from the State solely for those purposes expressly contemplated by the Agreement;
3. Not sell, rent, lease or disclose, or permit its employees, officers, agents, and independent contractors to sell, rent, lease, or disclose, any such PI to any third party, except as permitted under this Agreement or required by applicable law, regulation, or court order;
4. Take all commercially reasonable steps to (a) protect the confidentiality of PI received from the State and (b) establish and maintain physical, technical and administrative safeguards to prevent unauthorized access by third parties to PI received by Contractor from the State;
5. Give access to PI of the State only to those individual employees, officers, agents, and independent contractors who reasonably require access to such information in connection with the performance of Contractor's obligations under this Agreement;
6. Upon request by the State, promptly destroy or return to the State in a format designated by the State all PI received from the State;
7. Cooperate with any attempt by the State to monitor Contractor's compliance with the foregoing obligations as reasonably requested by the State from time to time. The State shall be responsible for all costs incurred by Contractor for compliance with this provision of this subsection;
8. Establish and maintain data security policies and procedures designed to ensure the following:
 - a) Security and confidentiality of PI;
 - b) Protection against anticipated threats or hazards to the security or integrity of PI; and
 - c) Protection against the unauthorized access or use of PI.

B. Disclosure to Third Parties. This Agreement shall not be deemed to prohibit disclosures:

1. Required by applicable law, regulation, court order or subpoena; provided that, if the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether PI or otherwise, pursuant to court or administrative order, subpoena, summons, or other legal process, Contractor will promptly notify the State (unless prohibited from doing so by law, rule, regulation or court order) in order that the State may have the opportunity to seek a protective order or take other appropriate action. Contractor will also cooperate in the State's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information provided by the State. If, in the absence of a protective order, Contractor is compelled as a matter of law to disclose the information provided by the State, Contractor may disclose to the party compelling disclosure only the part of such information as is required by law to be disclosed (in which case, prior to such disclosure, Contractor will advise and consult with the State and its counsel as to such disclosure and the nature of wording of such disclosure) and Contractor will use commercially reasonable efforts to obtain confidential treatment therefore;
2. To auditors or regulators;
3. To service providers and agents of either party as permitted by law, provided that such service providers and agents are subject to binding confidentiality obligations; or
4. To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

C. Limited Use; Survival of Obligations. Contractor may use PI only as necessary for Contractor's performance under or pursuant to rights granted in this Agreement and for no other purpose. Contractor's limited right to use PI expires upon expiration or termination of this Agreement for any

reason. Contractor's obligations of confidentiality and non-disclosure survive termination or expiration for any reason of this Agreement.

D. Disposal of PI. Upon expiration of Contractor's limited right to use PI, Contractor must return all physical embodiments to the State or, with the State's permission; Contractor may destroy PI. Upon the State's request, Contractor shall provide written certification to the State that Contractor has returned, or destroyed, all such PI in Contractor's possession.

E. Remedies. If Contractor or any of its representatives or agents breaches the covenants set forth in these provisions, irreparable injury may result to the State or third parties entrusting PI to the State. Therefore, the State's remedies at law may be inadequate and the State shall be entitled to seek an injunction to restrain any continuing breach. Notwithstanding any limitation on Contractor's liability, the State shall further be entitled to any other rights or remedies that it may have in law or in equity.

F. Disclosure Notification. If Contractor determines that there is any actual or suspected theft of, accidental disclosure of, loss of, or inability to account for any PI by Contractor or any of its subcontractors (collectively "Disclosure") and/or any unauthorized intrusions into Contractor's or any of its subcontractor's facilities or secure systems (collectively "Intrusion"), Contractor must immediately:

1. Notify the State within 24 hours of the Contractor becoming aware of the unauthorized disclosure;
2. Fully cooperate with the State in estimating the effect of the Disclosure or Intrusion's effect on the State and fully cooperate to mitigate the consequences of the Disclosure or Intrusion;
3. Specify corrective action to be taken;
4. Investigate and determine if an Intrusion and/or Disclosure has occurred; and
5. Take corrective action to prevent further Disclosure and/or Intrusion.

Contractor must, as soon as is reasonably practicable, make a report to the State including details of the Disclosure and/or Intrusion and the corrective action Contractor has taken to prevent further Disclosure and/or Intrusion. Contractor must, in the case of a Disclosure cooperate fully with the State to notify the effected persons as to the fact of and the circumstances of the Disclosure of the PI. Additionally, Contractor must cooperate fully with all government regulatory agencies and/or law enforcement agencies having jurisdiction to investigate a Disclosure and/or any known or suspected criminal activity.

8.13.4 Suspension and Termination

Notwithstanding anything in the Contract to the contrary, any time the State has the right to terminate the Contract, the State may elect to terminate the Contract only in part by notifying the Contractor of such decision. By electing to terminate only part of the Contract, the State does not give up its rights to later terminate other portions or the entire Contract. In the event the State terminates all or part of the Managed Services provided by the Contractor, the Contractor shall continue to be obligated to perform the services, both those that are to remain and those that are being terminated, in accordance with the requirements of the Contract, including without limitation, the service level requirements as long as the services continue to be provided. In addition, regardless of whether the termination is for all Managed Services or only part of the Managed Services, Contractor shall provide the transition services as set

forth in this RFP as necessary to enable the State to convert the Managed Services being terminated to another provider, including the State.

8.13.5 Telephone Numbers

Upon the termination of the Contract with respect to the Managed Services, any telephone numbers utilized in the performance of the Managed Services shall be transferred to the State. It shall be the responsibility of the Contractor to complete the transfer of the telephone numbers immediately upon the date the Managed Services are terminated. The telephone numbers shall be transferred to the State at no cost to the State. The telephone numbers that shall be transferred are those that the State transferred to the Contractor at the commencement of the Managed Services and all those telephone numbers acquired by the Contractor during the term of the Contract to enable the Contractor to perform its duties and obligations under the SOW for Managed Services.

8.13.6 Insurance

The Contractor shall provide to the State prior to commencement of the work following the award of the Contract, property insurance coverage to cover casualty loss of State's equipment in Contractor's possession up to replacement value of equipment. State shall be included on the CGL insurance policies obtained by Contractor as "Additional Insured". Such policies shall cover this Contract with respect to State's status as "Additional Insured" by way of a blanket additional insured endorsement and shall not specifically reference State by name. The provisions of this section shall not be deemed to limit or expand the liability of Contractor hereunder, or limit any rights that State may have including, without limitation, rights of indemnity or contribution. After insurance company determination to repair or replace, the proceeds, if any, from such property insurance based on loss or damage to the State's equipment will be applied to repair or replacement of that equipment, at the State's option.

8.13.7 Handling the State's Data

The Contractor must use due diligence to ensure computer and telecommunications systems and services involved in storing, using, or transmitting State Data are secure and to protect that data from unauthorized disclosure, modification, or destruction. "State Data" includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State. To accomplish this, the Contractor must adhere to the following principles:

1. Apply appropriate risk management techniques to balance the need for security measures against the sensitivity of the State Data.
2. Ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability.
3. Maintain plans and policies that include methods to protect against security and integrity threats and vulnerabilities, as well as and detect and respond to those threats and vulnerabilities.
4. Maintain appropriate identification and authentication process for information systems and services associated with State Data.
5. Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with State Data.

6. Implement and manage security audit logging on information systems, including computers and network devices.

The Contractor must maintain a robust boundary security capacity that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems that hold State Data, limiting access to only these points, and disable all others. To do this, the Contractor must use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available. The Contractor must use two-factor authentication to limit access to systems that contain particularly sensitive State Data, such as personally identifiable data.

Unless the State instructs the Contractor otherwise in writing, the Contractor must assume all State Data and information is both confidential and critical for State operations, and the Contractor's security policies, plans, and procedure for the handling, storage, backup, access, and, if appropriate, destruction of that data must be commensurate to this level of sensitivity. As part of the Contractor's protection and control of access to and use of State Data, the Contractor must employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access the State's Data, as well as attacks on the Contractor's infrastructure associated with the State's data. Further, the Contractor must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with the State's Data.

The Contractor must use appropriate measures to ensure that State Data is secure before transferring control of any systems or media on which State Data is stored. The method of securing the State Data must be appropriate to the situation and may include erasure, destruction, or encryption of the State Data before transfer of control. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under this Contract.

The Contractor must have a business continuity plan in place that the Contractor tests and updates at least annually. The plan must address procedures for response to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Contractor maintains the State's Data in case of loss of that data at the primary site. The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State's Data in the case of a disaster or other business interruption. The Contractor's business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to the State's Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Contractor also must provide for reviewing, testing, and adjusting the plan on an annual basis.

The Contractor may not allow the State's Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Contract

properly. Even then, the Contractor may permit such only if adequate security measures are in place to ensure the integrity and security of the State Data. Those measures must include a policy on physical security for such devices to minimize the risks of theft and unauthorized access that includes a prohibition against viewing sensitive or confidential data in public or common areas. At a minimum, portable computing devices must have anti-virus software, personal firewalls, and system password protection. In addition, the State's Data must be encrypted when stored on any portable computing or storage device or media or when transmitted from them across any data network. The Contractor also must maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

Any encryption requirement identified in this provision means encryption that complies with National Institute of Standards Federal Information Processing Standard 140-2 as demonstrated by a valid FIPS certificate number. Any sensitive State Data transmitted over a network, or taken off site via removable media must be encrypted pursuant to the State's Data encryption standard ITS-SEC-01 Data Encryption and Cryptography.

The Contractor must have reporting requirements for lost or stolen portable computing devices authorized for use with State Data and must report any loss or theft of such to the State in writing as quickly as reasonably possible. The Contractor also must maintain an incident response capability for all security breaches involving State Data whether involving mobile devices or media or not. The Contractor must detail this capability in a written policy that defines procedures for how the Contractor will detect, evaluate, and respond to adverse events that may indicate a breach or attempt to attack or access State Data or the infrastructure associated with State Data.

In case of an actual security breach that may have compromised State Data, the Contractor must notify the State in writing of the breach within 2 hours of the Contractor becoming aware of the breach and fully cooperate with the State to mitigate the consequences of such a breach. This includes any use or disclosure of the State data that is inconsistent with the terms of this Contract and of which the Contractor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this Contract by an employee, agent, or subcontractor of the Contractor.

The Contractor must give the State full access to the details of the breach and assist the State in making any notifications to potentially affected people and organizations that the State deems are necessary or appropriate. The Contractor must document all such incidents, including its response to them, and make that documentation available to the State on request. In addition to any other liability under this Contract related to the Contractor's improper disclosure of State data, and regardless of any limitation on liability of any kind in this Contract, the Contractor will be responsible for acquiring one year's identity theft protection service on behalf of any individual or entity whose personally identifiable information is compromised while it is in the Contractor's possession. Such identity theft protection must provide coverage for all three major credit reporting agencies and provide immediate notice through phone or email of attempts to access the individuals' credit history through those services."

To the extent the State requires the Contractor to adhere to specific processes or procedures in addition to those set forth above in order for the Contractor to comply with the managed services principles enumerated herein, those processes or procedures are set forth in this Managed Services SOW.